Proposing a New Foundation of Attack Trees in Monoidal Categories

Harley Eades III

Computer and Information Sciences, Augusta University, Augusta, GA,
heades@augusta.edu

Abstract. TODO

1 Introduction

Attack trees are a modeling tool, originally proposed by Bruce Schneier [17], which are used to assess the threat potential of a security critical system. Attack trees have since been used to analyze the threat potential of many types of security critical systems, for example, cybersecurity of power grids [19], wireless networks [16], and many others. Attack trees consists of several goals, usually specified in English prose, for example, "compromise safe" or "obtain administrative privileges", where the root is the ultimate goal of the attack and each node coming off of the root is a refinement of the main goal into a subgoal. Then each subgoal can be further refined. The leaves of an attack tree make up the set of base attacks. Subgoals can be either disjunctively or conjunctively combined.

Extensions of attack trees. There have been a number of extensions of attack trees to include new operators on goals. One such extension recasts attack trees into attack nets which have all of the benefits of attack trees with the additional benefit of being able to include the flaw hypothesis model for penetration testing [13]. A second extension adds sequential conjunction of attacks, that is, suppose A_1 and A_2 are attacks, then $A_1; A_2$ is the attack obtained by performing A_1, and then executing attack A_2 directly after A_1 completes [7].

The need for a foundation. Attack trees for real-world security scenarios can grow to be quite complex. The attack tree presented in [19] to access the security of power grids has twenty-nine nodes with sixty counter measures attached to the nodes throughout the tree. The details of the tree spans several pages of appendix. The attack tree developed for the border gateway protocol has over a hundred nodes [4], and the details of the tree spans ten pages. Manipulating such large trees without a formal semantics can be dangerous.

The formal semantics of attack trees. The leading question the field is seeking to answer by giving a mathematical foundation to attack trees is "what is an attack tree?" There have been numerous attempts at answering this question. For example, attack trees have been based on propositional logic and De Morgan Algebras [9,8,14], multisets [12], Petri nets [13], tree automata [3], and series parallel graphs [7]. **There is currently no known semantics of attack trees based in category theory**.

By far the most intuitive foundation of attack trees is propositional logic or De Morgan algebras, however, neither of these properly distinguish between attack trees with repeated subgoals. If we consider each subgoal as a **resource** then the attack tree using a particular resource twice is different than an attack tree where it is used only once. The multiset semantics of attack trees was developed precisely to provide a resource conscious foundation [12]. The same can be said for the Petri nets semantics [13]. A second benefit of a semantics based in multisets, Petri nets, and even tree automata is that operators on goals in attack trees are associated with concurrency operators from process algebra. That is, the goals of an attack tree should be thought of as being run concurrently – it seems this connection to process algebra has been overlooked. Furthermore, when moving to these alternate foundations **the intuitiveness and elegance of the propositional logic semantics is lost**. Lastly, existing work has focused on specifically what an attack tree is, and has not sought to understand what the theory of attack trees is.

Category Theory. Each of the various existing mathematical foundations attempt to answer the question "what is an attack tree?", but they are all seemingly very different mathematical structures. Is there a unifying core foundation common to all of these existing foundations? A categorical foundation will answer this question in the positive. The powers of category theory – an abstract branch of mathematics first proposed by Samuel Eilenberg and Saunders Mac Lane [11] – are its ability to abstract away unneeded details from a mathematical structure, and its ability to form relationships between seemingly unrelated mathematical structures. For example, intuitionistic logic and the λ-calculus both correspond to cartesian closed categories, and hence, are different perspectives of the same theory [10]. A categorical foundation of attack trees will result in the most basic mathematical foundation of attack trees, furthermore, it will reveal a relationship between all of the existing mathematical foundations, and lastly, it will reconnect attack trees with logic, but also forge new connections with functional programming languages and formal verification through the Curry-Howard-Lambek correspondence. This implies that by giving attack trees a semantics in category theory one obtains a more powerful semantic analysis and the ability to **derive a programming language that can not only define attack trees, but also reason about them using formal verification** (Section **??**). In addition, the various graphical languages used in category theory, [18], may lead to new graphical tools for threat analysis.

This Proposal. I propose to found attack trees in linear logic rather than propositional logic by giving attack trees a semantics in symmetric monoidal categories. A semantics in symmetric monoidal categories is a generalization over the previous forms of models of attack trees. Multisets and Petri nets are examples of symmetric monoidal categories [1,20]. Furthermore, symmetric monoidal categories are a categorical model of linear logic [6], thus regaining the elegant connection between attack trees and logical formulas. The connection to linear logic also opens the door to a connection between threat analysis using attack trees and process algebra such as Petri nets, but also Chu spaces [15], dialec-

tica spaces [5], and session types [21,2]. I and my trainees will fully develop the semantics of attack trees in symmetric monoidal categories and show that not only can attack trees be modeled by these types of categories, but so can a range of their extensions like attack trees with sequential conjunction. We will also investigate new attack tree operators based on the connection to process algebra. Then we will develop a new formal system called Lina for Linear Threat Analysis (Section **??**). Lina will be a statically typed linear polymorphic functional domain-specific programming language designed to construct, manipulate, and prove properties of attack trees. Lina will represent attack trees as linear types, and thus, programs between these types will be considered transformations of attack trees. The semantics of Lina will also be in symmetric monoidal categories forming a tight correspondence with the semantics of attack trees. This system will be the first threat analysis tool to support proving properties of attack trees, thus **connecting software verification to threat analysis.** Finally, new threat analysis tools can be built on top of Lina.

References

1. Carolyn Brown, Doug Gurr, and Valeria Paiva. A linear specification language for petri nets. *DAIMI Report Series*, 20(363), 1991.
2. LuÃ-s Caires and Frank Pfenning. Session types as intuitionistic linear propositions. In Paul Gastin and FranÃ§ois Laroussinie, editors, *CONCUR 2010 - Concurrency Theory*, volume 6269 of *Lecture Notes in Computer Science*, pages 222–236. Springer Berlin Heidelberg, 2010.
3. S.A. Camtepe and B. Yener. Modeling and detection of complex attacks. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, pages 234–243, Sept 2007.
4. S. Convery, D. Cook, and M. Franz. An attack tree for the border gateway protocol. 2003. `https://tools.ietf.org/html/draft-ietf-rpsec-bgpattack-00`.
5. Valeria de Paiva. Dialectica and chu constructions: Cousins? *Theory and Applications of Categories*, 17(7):127–152, 2006.
6. Valeria de Paiva. Categorical semantics of linear logic for all. In Luiz Carlos Pereira, Edward Hermann Haeusler, and Valeria de Paiva, editors, *Advances in Natural Deduction*, volume 39 of *Trends in Logic*, pages 181–192. Springer Netherlands, 2014.
7. Ravi Jhawar, Barbara Kordy, Sjouke Mauw, SaÅ!'a RadomiroviÄ, and Rolando Trujillo-Rasua. Attack trees with sequential conjunction. In Hannes Federrath and Dieter Gollmann, editors, *ICT Systems Security and Privacy Protection*, volume 455 of *IFIP Advances in Information and Communication Technology*, pages 339–353. Springer International Publishing, 2015.
8. Barbara Kordy, Marc Pouly, and Patrick Schweitzer. Computational aspects of attack–defense trees. In Pascal Bouvry, MieczysławA. Kłopotek, Franck Leprévost, Małgorzata Marciniak, Agnieszka Mykowiecka, and Henryk Rybiński, editors, *Security and Intelligent Information Systems*, volume 7053 of *Lecture Notes in Computer Science*, pages 103–116. Springer Berlin Heidelberg, 2012.
9. Barbara Kordy, Marc Pouly, and Patrick Schweitzer. A probabilistic framework for security scenarios with dependent actions. In Elvira Albert and Emil Sekerinski, editors, *Integrated Formal Methods*, volume 8739 of *Lecture Notes in Computer Science*, pages 256–271. Springer International Publishing, 2014.

10. J. Lambek. From lambda calculus to cartesian closed categories. *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 376–402, 1980.
11. Saunders Mac Lane. *Categories for the Working Mathematician.* Number 5 in Graduate Texts in Mathematics. Springer-Verlag, 1971.
12. Sjouke Mauw and Martijn Oostdijk. Foundations of attack trees. In DongHo Won and Seungjoo Kim, editors, *Information Security and Cryptology - ICISC 2005*, volume 3935 of *Lecture Notes in Computer Science*, pages 186–198. Springer Berlin Heidelberg, 2006.
13. J. P. McDermott. Attack net penetration testing. In *Proceedings of the 2000 Workshop on New Security Paradigms*, NSPW '00, pages 15–21, New York, NY, USA, 2000. ACM.
14. L. Piètre-Cambacédès and M. Bouissou. Beyond attack trees: Dynamic security modeling with boolean logic driven markov processes (bdmp). In *Dependable Computing Conference (EDCC), 2010 European*, pages 199–208, April 2010.
15. Vaughan Pratt. Chu spaces. Notes for the School on Category Theory and Applications University of Cimbra, July 1999.
16. A. Reinhardt, D. Seither, A. Konig, R. Steinmetz, and M. Hollick. Protecting ieee 802.11s wireless mesh networks against insider attacks. In *Local Computer Networks (LCN), 2012 IEEE 37th Conference on*, pages 224–227, Oct 2012.
17. Bruce Schneier. Attack trees: Modeling security threats. *Dr. Dobb's journal*, December 1999.
18. Peter Selinger. A survey of graphical languages for monoidal categories. *ArXiv e-prints*, August 2009.
19. Chee-Wooi Ten, Chen-Ching Liu, and Manimaran Govindarasu. Vulnerability assessment of cybersecurity for scada systems using attack trees. In *Power Engineering Society General Meeting, 2007. IEEE*, pages 1–8, June 2007.
20. A Tzouvaras. The linear logic of multisets. *Logic Journal of IGPL*, 6(6):901–916, 1998.
21. Philip Wadler. Propositions as sessions. In *Proceedings of the 17th ACM SIGPLAN International Conference on Functional Programming*, ICFP '12, pages 273–286, New York, NY, USA, 2012. ACM.